REMARKS

The Office Action mailed on April 12, 2006 has been received and reviewed. Claims 1-30 are in the case. Claims 1-3, 5-6, 13-16, 18-19, 20-23, and 25-29 were rejected under 35 U.S.C. 102(b) as being anticipated by Hardjono (6,425,004). Claims 7-9 and 11-12 were rejected under 35 U.S.C. 103(a) as being unpatentable over Hardjono (6,425,004) in view of *Microsoft Computer Dictionary* (Microsoft). Claims 4, 17, 24, 30 were rejected under 35 U.S.C. 103(a) as being unpatentable over Hardjono (6,425,004) in view of Goldberg et al. (US2003/0115516). Claim 10 was rejected under 35 U.S.C. 103(a) as being unpatentable over Hardjono (6,425,004) in view of *Microsoft Computer Dictionary* (Microsoft) in further view of Goldberg et al. (US2003/0115516).

In light of the rejections, a review of the present invention may help clarify the novelty of the Applicants' claims over the cited prior art. The present invention enables identification of a faulty communication module in a data storage system by error isolation. A computer host generates a data packet and an associated data verification value, preferably using cyclic redundancy check (CRC), and sends it to a storage module through a communication module. The communication module verifies the data in the packet. The communication module further associates a self identifier and a second data verification value, preferably using longitudinal redundancy check (LRC), with the data packet. The storage module stores the data packet.

A validation module retrieves the data packet from the storage module. The validation module first attempts to validate the second data verification value then, upon success, attempts to validate the first data verification value. If the validation module validates the second data verification value but not the first data verification value, the communication module is identified via the self identifier as faulty. Based on the sequence of discovery of the corrupt packet, the identity of the faulty communication module is easily ascertained from the self identifier associated with the data packet. The validation module may then communicate the identity of the faulty communication module to the storage module. And the storage module 204 may attempt to fix or take the faulty

communication module off-line. Using a (self) identifier that is inherent to the communication module facilitates location of a faulty device without requiring additional equipment to manage or distribute unique identifiers.

Applicants assert that the cited prior art is not enabling with regards to the present invention. For example, Hardjono is directed toward detecting faulty packets in a network. Specifically, Hardjono discloses dividing all domains in a network into sectors identified with sector tags, and all devices in each sector identified with device tags (see Hardjono, Figure 1). In this regard, Hardjono requires at least one domain controller or server to be present, and requires ongoing management of those domains. When a device sends a data packet, the device associates a device tag and the authenticating device for a sector associates a sector tag to the data packet. Each tag comprises the corresponding key and the data computed using a one-way hash. The device tag further includes the sector tag in the one-way hash.

When the data packet is received, the receiving device or receiving STA attempts to validate the sector tag by acquiring the sector key from a sector key table. If the sector tag is valid the receiving device or receiving STA attempts to validate the device tag. The device tag is validated by obtaining an apparently random device key and computing the one-way hash with the device key, sector tag, and data. If the result matches the device tag, an authentic originating device has been found; but if the result does not match, the process repeats until an authentic device is found (Hardjono, column 9, lines 8-14). In attempting to filter out invalid packets, Hardjono follows an authentication method which either accepts or drops packets according to selected information, such as sector keys and sector tags.

In reference to Goldberg, both CRC and LRC data verifications are disclosed to detect errors. Goldberg references both redundancy checks as two of a "variety of techniques to detect errors" (Goldberg, paragraph 0032). Goldberg later recognizes that a network may "simultaneously employ many different techniques and processes to provide error detection" (paragraph 0032). The reference

to Goldberg is limited to the above references without further explanation of the techniques and processes capable of providing error detection.

Regarding the rejection of claims 1-3, 5-6, 13-16, 18-19, 20-23, and 25-29 under 35 U.S.C. 102(b) as being anticipated by Hardjono (6,425,004) and claims 7-9 and 11-12 under 35U.S.C. 103(a) as being unpatentable over Hardjono in view of *Microsoft Computer Dictionary*. Hardjono does not disclose nor enable utilizing an inherent identifier associated with the device as a unique identifier for the device. Rather practicing Hardjono requires configuring sectors from a domain then assigning device and sector keys. Furthermore, Hardjono attempts to authenticate the sector key and sector tag to determine whether to accept or drop a packet. Consequently, Hardjono is directed to authentication of packets rather than isolation of a faulty communication module. Also, neither the device key nor the sector key is apparently inherent, such as a hardware address or abstraction of the hardware address would be. Finally, the authentication method or Hardjono which uses the sector key and sector tag to determine whether to accept or drop a packet differs from the error isolation method of the present invention.

Specifically, Hardjono does not teach executing first and second data verification checks to strategically validate a data packet while identifying a faulty communication module. Hardjono merely utilizes any one-way hash function in their authentication method to verify valid data packets. Furthermore, no stratagem is involved in the use of the one-way hash function which results in a trial-and-error methodology to discover if the packet is authentic. In contrast, the present invention strategically appends a first check value by a source device. A unique identifier and second check value are appended to a packet by an intermediate device. This approach enables easy identification of both a corrupt data packet and a faulty intermediate device.

Regarding the rejection of claims 4, 17, 24, 30 under 35 U.S.C. 103(a) as being unpatentable over Hardjono in view of Goldberg, Applicants assert that the cited prior art fails to disclose executing first and second verifications to strategically validate a data packet while identifying a faulty communication module. Applicants acknowledge that Goldberg teaches a communication

module configured to verify data using the longitudinal redundancy check for a data packet; however, Applicants assert that the novelty of their invention is not the addition of second redundancy check to identify an error in the data packet, but it is the strategic execution of second redundancy check by an intermediate communication module on the data packet and a unique identifier that enables the identification of not only the data error, but also the specific device that provided the error. Applicants acknowledge that Goldberg does teach LRC data verification in a network, but it fails to disclose strategically executing a first and second redundancy check to detect a data error and identify the faulty device.

CONCLUSION

In summary, while the use of CRC and LRC data verifications are well known in the prior art, the ability to determine a data error and identify a faulty intermediate device is a novel aspect of the present invention. Additionally, the use of an identifier that is inherently specific to the device such as a "hardware address or an abstraction of the hardware address" (Benhase, paragraph 0060) allows the faulty device to be directly identified without requiring the use of a domain controller or the like. Applicants again reiterate that neither of these teachings are disclosed or anticipated in the cited prior art. Applicants therefore assert that the combination of elements cited in Applicants' claims is novel and non-obvious.

For the reasons stated above, Applicants assert that claims 1-30 are in condition for allowance and respectfully request prompt allowance of the pending claims. In the event that the Examiner finds any remaining impediments to the prompt allowance of any of these claims which could be clarified in a telephone conference, the Examiner is respectfully urged to initiate the same with the undersigned.

Respectfully submitted,

Date: September 12, 2006

/Brian C. Kunzler/

Kunzler & Associates
8 E. Broadway, Suite 600
Salt Lake City, Utah 84111
Telephone: 801/994-4646

Brian C. Kunzler
Reg. No. 38,527
Attorney for Applicant